Introducción a la Teoría de Códigos

M.A. García, L. Martínez, T. Ramírez

Facultad de Ciencia y Tecnología. UPV/EHU

Resumen Teórico
Apartado 5 del Tema 2: Códigos equivalentes

Mayo de 2017

5 Códigos equivalentes

Cuando consideramos dos códigos de bloque C_1 y C_2 con la misma longitud n sobre el mismo alfabeto A nos interesará no solo que C_1 y C_2 sean diferentes como subconjuntos de T_n, sino que también nos preocuparemos de que las capacidades correctoras de ambos u otras características intrínsecas a ellos sean diferentes. Por ello, vamos a introducir la definición de códigos equivalentes que va a recoger esta idea. Necesitamos primero introducir dos tipos de aplicaciones de T_n en sí mismo:

1. Sean $i, j \in \{1, \ldots, n\}$ con $i < j$. Se define

$$\begin{array}{cccc} \phi_{ij}: & T_n & \to & T_n \\ & x_1 \ldots x_n & \mapsto & x_1 \ldots x_{i-1} x_j x_{i+1} \ldots x_{j-1} x_i x_{j+1} \ldots x_n. \end{array}$$

   Es decir, ϕ_{ij} intercambia las letras que aparecen en las posiciones i y j de cada palabra $\mathbf{x} \in T_n$.

2. Dada una permutación $g : A \to A$, esto es, g es una aplicación biyectiva de A en sí mismo, y un índice $k \in \{1, \ldots, n\}$, se define

$$\begin{array}{cccc} \psi_{g,k}: & T_n & \to & T_n \\ & x_1 \ldots x_n & \mapsto & x_1 \ldots x_{k-1} g(x_k) x_{k+1} \ldots x_n. \end{array}$$

   Esto es, $\psi_{g,k}$ lo que hace es aplicar la permutación g a las letras que aparecen en la posición i-ésima.

Definición Sea A un alfabeto y $C_1, C_2 \subseteq T_n$. Se dice que C_2 es **equivalente** a C_1, si se puede obtener C_2 como la imagen de C_1 mediante una aplicación h, que es la composición de un número finito de aplicaciones del tipo ϕ_{ij} y $\psi_{g,k}$ para $g \in \Sigma_A$ y $i, j, k \in \{1, \ldots, n\}$.

Observamos que al ser tanto las aplicaciones del tipo ϕ_{ij} como $\psi_{g,k}$ biyectivas con inversa del mismo tipo es evidente que si C_2 es equivalente a C_1, entonces C_1 es equivalente a C_2. Por tanto, diremos simplemente que C_1 y C_2 son equivalentes. Además, si consideramos $\mathcal{T}_n$ el conjunto de los códigos de longitud n sobre el alfabeto A, se tiene que el ser equivalentes es una relación de equivalencia en $\mathcal{T}_n$, que denotamos por $\mathcal{R}$. Podemos calcular el conjunto cociente $\mathcal{T}_n/\mathcal{R}$ y la clase de un código $C \in \mathcal{T}_n$ vendrá dada por:

$$[C] = \{C_2 \mid C \mathcal{R} C_2\}.$$

Una propiedad interesante de los códigos equivalentes es la que relaciona las distancias mínimas de los códigos equivalentes y que la resumimos en la siguiente Proposición:

Proposición 5.1 *Sea $C_1 \subseteq T_n$ un código de longitud n sobre el alfabeto A y distancia mínima d. Si $C_2 \subseteq T_n$ es un código equivalente a C_1, entonces la distancia mínima de C_2 es también d.*

Para demostrar la Proposición anterior basta fijarse que si elegimos $\mathbf{x}, \mathbf{y} \in T_n$, se cumple

1. $d(\mathbf{x}, \mathbf{y}) = d(\phi_{ij}(\mathbf{x}), \phi_{ij}(\mathbf{y}))$
2. $d(\mathbf{x}, \mathbf{y}) = d(\psi_{g,k}(\mathbf{x}), \psi_{g,k}(\mathbf{y}))$

Por otro lado, si nos fijamos en la Proposición anterior, podemos deducir que una condición necesaria para que dos códigos de bloque de longitud n con alfabeto A sean equivalentes es que ambos tengan la misma distancia mínima.

Por otro lado, se puede demostrar la siguiente proposición:

Proposición 5.2 *Sea $C_1 \subseteq T_n$ un código de longitud n y $\boldsymbol{u} \in T_n$. Entonces, existe $C_2 \subseteq T_n$ equivalente a C_1 tal que $\boldsymbol{u} \in C_2$.*

Como consecuencia del resultado anterior, deducimos que

Corolario 5.3 *Sea $C_1 \subseteq \mathbb{F}_q^n$ un código de longitud n. Entonces, existe $C_2 \subseteq \mathbb{F}_q^n$ equivalente a C_1 tal que $00\ldots00 \in C_2$.*

Esto será interesante cuando deseemos construir un código de bloque de longitud n sobre $\mathbb{F}_q$ que contenga al $0\ldots0$ y sea equivalente a uno dado $C_1 \subseteq \mathbb{F}_q^n$, que no contiene al $0\ldots0$.